REMARKS

Applicant has amended Claim 10 to overcome the examiner's objection and has amended claims 11 and 12 to clarify the subject matter of those claims.

35 U.S.C §101

The examiner rejected Claim 1 under 35 U.S.C. 101. The examiner reasons that:

> **the claim is rejected "because it is directed to a data structure ("A memory for storing a data structure for tracking network behavior, comprising: a connection table ...". When nonfunctional descriptive material is recorded on some memory, it is not statutory since no requisite functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a memory, does not make it statutory.**

Applicant disagrees. Claim 1 is statutory because it is directed to a novel manufacture, a memory, which is a manufacture under 35 U.S.C. 101. Claim 1 is consonant with the Federal Circuit's decision and in, *In re Lowry*, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994). In *Lowry* the court specifically found that:

> The Board reversed the 35 U.S.C. Section 101 rejection. The Board found that claims 1 through 5, directed to a memory containing stored information, as a whole, recited an article of manufacture. The Board concluded that the invention claimed in claims 1 through 5 was statutory subject matter. Lowry 32 F.3d at

In *Lowry*, the claims were found statutory by the Board because the claims were to a memory, i.e., an article of manufacture. The Board acknowledged the statutory nature of the memory, but then proceeded to apply the so-called printed matter doctrine. The printed matter rejection of the Board was subsequently reversed by the Federal Circuit. Applicant's claim 1 recites an article of manufacture, namely "A memory device storing a data structure for tracking network behavior." The Patent Office's own guidelines for patenting of Computer related inventions does not support the position taken by the examiner.[1]

[1] "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data. Both types of "descriptive material" are nonstatutory when claimed as descriptive material per

Claim 1 does not claim nonfunctional descriptive materials such as music, literary works and a compilation or mere arrangement of data. Rather, claim 1 claims a memory device storing a data structure for tracking network behavior including the novel feature of a connection table that maps each node of a network to a record object that stores information about traffic to or from the node and between that node and others nodes in the network. Claim 1 and claims dependent thereon are thus clearly drawn to statutory subject matter.

Double Patenting

The examiner provisionally rejected Claims 1-17 on the ground of non-statutory, obviousness-type double patenting as being unpatentable over claims 1-22 of co-pending Application No. 10701154 and claims 1-36 of co-pending Application No. 10701356.

The examiner stated:

> **Although the conflicting claims are not identical, they are not patentably distinct from each other a comparison between instant application independent claim 1 and the claims 1 and 14 (of the copending application number 10701154) and claims 1, 19, and 25 (of the copending application number 10701356) reveal the copending claims are simply species of the broader claim 1 of the instant application. Hence, claim 1 of the instant application is generic to the species of the invention covered by independent claims of the copending applications stated above. Thus, the broad generic invention is anticipated by the narrower species of the co-pending invention, thus without a terminal disclaimer, the species claims preclude issuance of the generic application. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993).**

Present Application 10/701,155

Claim 1 of the present application is reproduced below: 1. A memory device storing a data structure for tracking network behavior, comprising:

---

se. Warmerdam, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 158384, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994) (claim to data structure stored on a computer readable medium that increases computer efficiency held statutory) and Warmerdam, 33 F.3d at 1360-61, 31 USPQ2d at 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process claim) with Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory). MANUAL OF PATENT EXAMINING PROCEDURE §2106 page 2100-12 rev. May 20.04

a connection table that maps each node of a network to a record object that stores information about traffic to or from the node and between that node and others nodes in the network.

Co-pending Application 10/701,154

Claim 1 of the '154 matter is reproduced below:

1. A system, comprising:
a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network; and
an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to or from the node, with the aggregator device further comprising:
a process executed on the aggregator device to detect anomalies in connection patterns; and
a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

Co-pending Application 10/701,356

Claim 1 of the '356 matter is reproduced below:

1. A device, comprising:
a processor;
a memory storing:
a connection table that maps each node of a network to a host object, the connection table stores information about traffic to or from the node; and
a process to detect anomalies based on information in the connection table and to aggregate the anomalies into the network events according to connection patterns.

Claim 1 of the present application is directed to memory device that stores a data structure for tracking network behavior. In contrast claim 1 of co-pending application '154, is directed to a system that includes a plurality of collector devices ... an aggregator device that

receives the connection information from the plurality of collector devices ... a process ... to detect anomalies in connection patterns and a process ... to aggregate detected anomalies into the network events ... .

Also, in contrast claim 1 of co-pending application '356 is directed to a device including a processor, a memory storing a connection table that maps each node of a network to a host object, the connection table stores information about traffic to or from the node and a process to detect anomalies based on information in the connection table and to aggregate the anomalies into the network events according to connection patterns.

Claim 1 of the instant application is directed to a data structure that stores a connection table. In contrast, claim 1 of the co-pending application '154 is directed to a technique that aggregates detected anomalies into network events that can correspond to denial of service attack and scanning attack anomalies. Also, in contrast, claim 1 of the co-pending application '356 is directed to detecting anomalies based on information in the connection table and aggregating the anomalies into the network events according to connection patterns.

The mere use of a connection table as elements in the claims of the co-pending application does not make the claims in the instant application either anticipated by or obvious over the sets of claims of the co-pending applications because each of the sets of claims are directed to patentably distinct subject matter.

Therefore, the rejection is improper and should be removed.

35 U.S.C §102

The examiner rejected Claims 1-9 and 11-17 under 35 U.S.C. 102(e) as being anticipated by Tams et al U.S. Publication Number (20030069952), " Tams."

The examiner stated:

> **As per claim 1, Tams (20030069952) teaches a memory device (fig. 2, 162) storing a data structure for tracking network behavior (¶ 0079-0081 and ¶0198), comprising:**
>
> **a connection table (fig, 2, data table and Table 2, page 11) that maps each node of a network to a record object that stores information about traffic to or from the node and between that node and others nodes in the network (¶0157-0164 and ¶0210. See TABLE 2, page 11).**

Claim 1, which is directed to a memory device storing a data structure for tracking network behavior, is neither described nor suggested by Tams. Claim 1 includes the feature of "a connection table that maps each node of a network to a record object that stores information about traffic to or from the node and between that node and other nodes in the network."

The claimed record object feature of the memory of claim 1 is not suggested by any of the passages referred to by the examiner or elsewhere in Tams. Tams, for instance, whether in table 2 or the other tables, does not provide any mechanism to map each node of a network to a record object that stores information ... to or from the node and between that node and other nodes in the network."

The examiner argues that: Tams teaches: "**a connection table (fig, 2, data table and Table 2, page 11)** ...." Applicant disagrees. The data table referred to in Tams does not store the claimed record objects (or an equivalent) ... that stores information about traffic to or from the node and between that node and others nodes in the network.", but rather stores information from probe devices, that is, packet counts and byte counts.[2]

The table 2 on page 11 of Tams while showing IP addresses, and counters, does not "map[s] each node of a network to a record object." Rather, the table 2 is a listing of the different application protocols and packet/byte counts for those protocols.

The examiner also argues Tams teaches: **"maps each node of a network to a record object that stores information about traffic to or from the node and between that node and others nodes in the network (¶0157-0164 and ¶0210. See TABLE 2, page 11."** Applicant disagrees. Tams in these paragraphs discusses different ordering options for the contents of "alMartixTopN" table. However, this table (a version of which is depicted in table 2) does not "map[s] each node of a network to a record object that stores information about traffic to or from the node and between that node and others nodes in the network." In table 2, these entries are merely entries of source, destination addresses and counters. However, these entries are not mapped to a record object that stores information about traffic to or from the node and between that node and others nodes in the network.

Accordingly, claim 1 is allowable over Tams.

---

[2] Tams [0023].

Claims 2-5

The examiner rejected claims 2-5 arguing that:

> **As per claims 2 and 3, Tams teaches wherein the connection table includes a plurality of records that are indexed by source and destination address (See TABLE 2, page 11).**
>
> **As per claim 4, Tams teaches the device of claim 1 wherein the connection table includes a plurality of records that are indexed by time (¶0198 and ¶0201-0206; see steps in fig. 8).**
>
> **As per claim 5, Tams teaches the device of claim 1 wherein the connection table includes a plurality of records that are indexed by source address, destination address and time (See TABLE 2, page 11 and ¶0198 and ¶0201-0206).**

Each of claims 2-5 serves to further distinguish the claims over Tams. Claim 5 includes each of the features of claims 2-4 and therefore for brevity, Applicant will argue claim 5. However, it is understood that the other claims are equally distinct over Tams.

Claim 5 recites that: "... the connection table includes a plurality of records that are indexed by source address, destination address and time." For the table being indexed by source and destination address the examiner argues: "... **(See TABLE 2, page 11).**" Table 2, page 11 does not show a table indexed by source address or by destination address, but merely that the table has source and destination addresses stored therein for a particular entry.

As for indexing by time, the examiner argues: **(See TABLE 2, page 11 and ¶0198 and ¶0201-0206)**: Applicant also disagrees. No indexing by time is disclosed in the cited passages. Rather, the cited passages disclose: At 0198 Tams discloses a network traffic database that stores network traffic at different resolutions (time), but stored in FIFO's. There is no mention made of indexing by time and storage is of datasets that overlap in time. Indeed, throughout **¶0201-0206)** Tams fails to mention indexing by time, but instead is directed to updating entries in the parallel data sets.

As for claims 6-11, Tams does not teach the base features of the "the connection table" and does not teach therefore that the connection table is arranges as "sub-tables" over different time scales.

As for claim 11, the examiner argues: "**... Tams teaches the device of claim 1 wherein the host record of a first host also maps to a second host which communicates with the first host to a "host pair record" that has information about all the traffic from between the first and second hosts (¶0201 and ¶0209-0210).**" Tams does not suggest the features that: "the host record of a first host maps to a second host that

communicates with the first host to a "host pair record object" that has information about all the traffic from the first to the second host and from the second host to the first host."

As for claim 12, the examiner argues: "**...Tams teaches the device of claim 1 wherein connection data structure enables a consuming device to obtain summary information about one bost and about tbe traffic between any pair of bosts, in eitber direction (10118).**" Applicant disagrees. Claim 12 includes the features of "wherein the connection table includes two level mapping that enables a consuming device to obtain summary information about one host for a first level mapping and about the traffic between any pair of hosts, in either direction, between a first one of the hosts of the any pair to a second one of the hosts of the any pair and from the second one of the hosts of the any pair to the first one of the hosts of the any pair for a second level mapping." No such arrangement is taught by Tams.

Claims 13-17 are allowable over Tams at least for the reasons discussed in claim 1.

35 U.S.C §103

The examiner rejected Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tams in view of Maufer et al U.S. Patent Number (7,120,930), " Maufer".

The examiner argues:

> **As per claim 10, although Tams shows substantial features of the claimed invention including a table with plurality of records, he does not explicitly show a physical [layer] address to IP address map that is used to determine Host ID. Nonetheless, this feature is well known in the art and would have been an obvious modification of the system disclosed by Tams, as evidenced by Maufer U.S. Patent Number (7120930).**
>
> **In analogous art, Maufer whose invention is about a Method and apparatus for enbanced security for communication over a network including a mapping table accessible by a gateway computer used to form associations between a local address for the client and a destination address for a peer and a Security Parameters Index associated with IPSec-protected traffic from the peer (abstract), discloses a physical [layer] address to IP address map that is used to determine Host ID (col. 16, line 51-65 and table 300, fig. 5A. See also col. 5, lines 36-60).**
>
> **Giving the teacbing of Maufer, a person of ordinary skill in the art would bave readily recognized tbe advantage of modifying Tams by employing tbe enhanced network security system of Maufer for particularly identifying traffic flowing from a remote address to tbe local address using pbysical layer (MAC) address to IP address mapping in order to verify hosts belonging to the private network from unknown intruders of the public network. In this way fake packets belonging to unknown sources are recognized and discarded.**

Claim 10 includes the feature that "the addresses indexing the connection include a physical layer address to IP address map that is used to determine Host ID."

Applicant contends that no combination of Tams with Maufer suggests the features of claim 10. Maufer does not teach "the addresses indexing the connection include a physical layer address to IP address map that is used to determine Host ID" as the examiner argues but instead discloses mapping between active clients and gateway managed public IP addresses. However, while discussing mapping, Maufer clearly does not teach any mapping for use in a connection table of the type claimed in claim 1 for the function to determine Host ID in the connection table.

Applicant has enclosed herewith an Information Disclosure Statement. Applicant contends that the art of record when taken separately or in combination with the art in the enclosed information disclosure statement neither describes nor suggests Applicant's claimed invention.

Please charge the Petition for Extension of Time fee of **$60** and please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 12/21/07

Dennis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906